CHAPTER 1

概要

この章では、Cisco Application Content Networking System（ACNS）ソリューションの概要を説明します。この章の構成は、次のとおりです。

（注） このマニュアル全体で「スタンドアロン Content Engine」という用語は、Content Engine をスタンドアロン デバイスとして設定、管理、および監視できるようにするために、ACNS 管理者が意図的に Content Distribution Manager（ネットワーク内にある場合）に登録しなかった Content Engine を指すために使用されます。このマニュアルでは、ACNS ソフトウェア 5.3.x を実行しているスタンドアロン Content Engine の配置、管理、また監視について特別に焦点を合わせています。スタンドアロン Content Engine を複数配置できます（たとえば、スタンドアロン Content Engine クラスタ構成で配置することもできます）。スタンドアロン Content Engine を設定するには、Content Engine CLI、Content Engine GUI、または ACNS 5.2.1 ソフトウェア リリースで導入された Setup ユーティリティを使用することができます。

Content Distribution Manager に登録された Content Engine を配置、管理、監視する方法については、『中央管理配置に関する Cisco ACNS ソフトウェア コンフィギュレーション ガイド , Release 5.3』を参照してください。

ACNS ソフトウェア ソリューションの概要

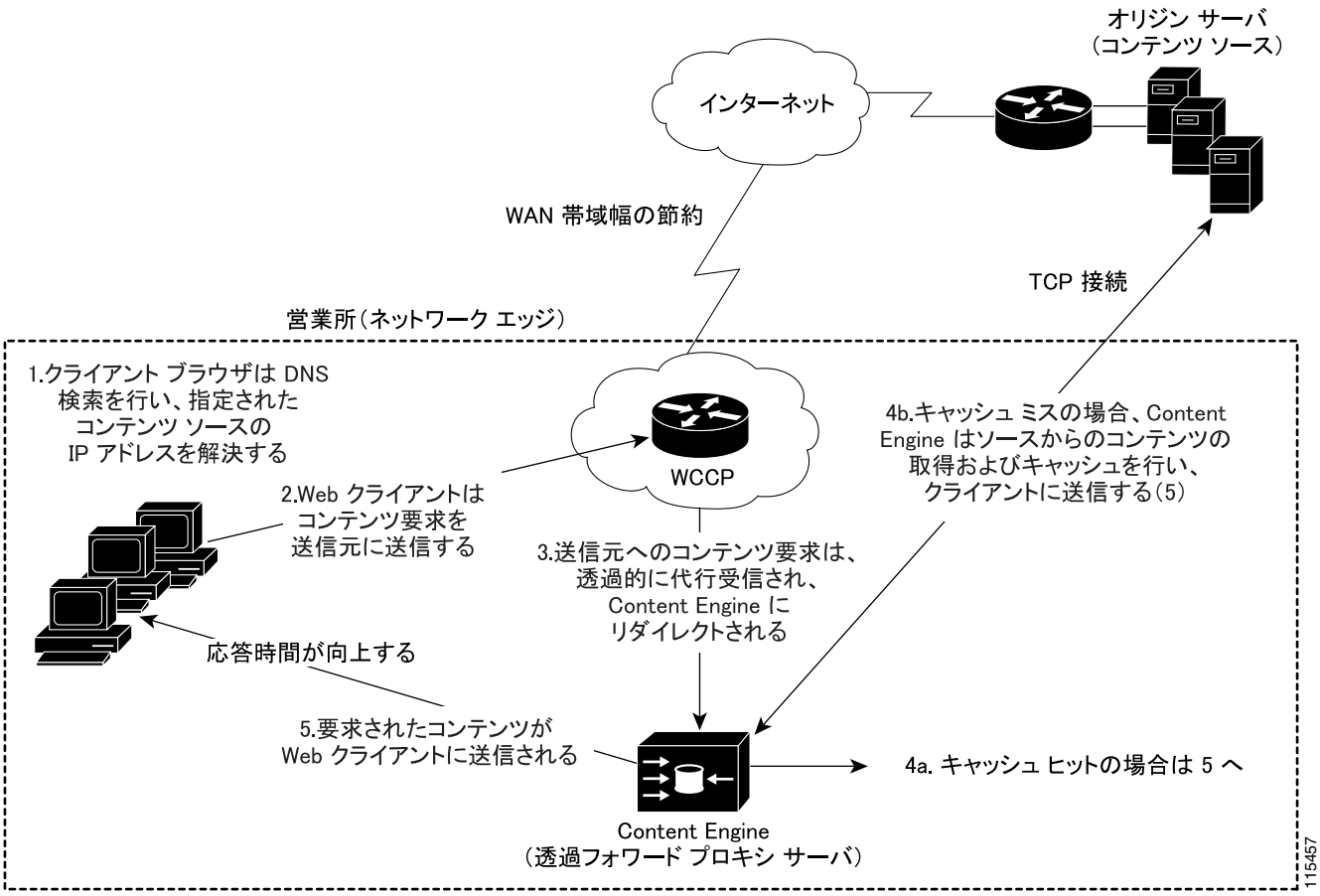
e- コマース、e- ラーニング、知識共有、企業通信などの e-business アプリケーションが出現するにつれ、ネットワークでトラフィックのフローに関して制御不能なボトルネックを経験することがあります。ACNS ソリューションは、企業やインターネット サービス プロバイダー（ISP）が、ネットワークがボトルネックにより、制御不能な障害から保護し、数多くのメディア ファイルをエンドユーザに効率的に配信するのに役立ちます。手頃な値段と容易なインストレーションのために設計された ACNS ソリューションは、最小の管理で迅速に配置することで高品質のストリーミング ビデオなどの、インパクトの大きな広帯域幅で メディアを短時間で配信することを可能にします。ストリーミングとは、すべてのメディア パケットを受信し終わる前に、コンテンツにアクセスまたはコンテンツを表示できる技術です。キャッシングではコンテンツをアクセス可能にする前にコンテンツ全体を受信しておく必要があります。

ACNS ソフトウェアでは、複数のコンテンツ ルーティング方式をサポートして、複数の方法で Content Engine のキャッシュにコンテンツが取り込まれるように考慮しています。ACNS ソフトウェアを組み込んだ Cisco Content Engine は、頻繁にアクセスされるコンテンツを透過的またはプロキシスタイルでキャッシングし、コンテンツ要求をインターネットやイントラネットを横断して遠隔地にあるサーバにアクセスするよりもローカル側で満たすことにより、コンテンツ配信を高速化します。

コンテンツをローカル側にキャッシュすることにより、Content Engine は WAN リンクを横断する冗長なネットワーク トラフィックを最小限にします。その結果、WAN 帯域幅コストが削減されるか、あるいはコストの増加が緩やかになります。このように帯域幅を最適化することにより、追加ユーザまたは追加トラフィックに使用できるネットワーク容量が増加し、また Voice over IP（VoIP）などの新規サービス用のネットワーク容量も増加します。

たとえば、企業は 1 台またはそれ以上の Content Engine を各営業所に配置し、各 Content Engine のアクセス コントロールとフィルタリングを設定した後、これらの Content Engine にコンテンツをプッシュできます。各営業所の Content Engine は特定のポリシーを使用して、コンテンツ要求を拒否するか、受け入れるかを判断します。コンテンツに対するアクセスが受け入れられると、Content Engine は、そのコンテンツのコピーがローカルにキャッシュされているかどうかをチェックします。コンテンツがすでにローカル キャッシュに保管されている場合、Content Engine はクライアントにキャッシュされているコンテンツを送信します。それ以外の場合は、コンテンツをソース（オリジン サーバ）から取得し、コンテンツをキャッシュし、このキャッシュされたコンテンツをクライアントに送信します。Content Engine は、これ以降クライアントから同一コンテンツを要求されると、Content Engine はオリジン サーバから再度コンテンツを取得するのではなく、クライアントにキャッシュされたコンテンツを送信します。配置例については、図 1-1 を参照してください。

図 1-1　営業所におけるスタンドアロン Content Engine の大規模な配置例



この配置例では、クライアントの要求は、Cisco の Web Cache Communication Protocol（WCCP）を実行しているルータにより、営業所の Content Engine に透過的にリダイレクトされています。他に考えられるルーティング方式には、レイヤ 4 Cisco Content Services Switch（[CSS] スイッチ）を介した透過的なリダイレクト、または、直接プロキシ ルーティング（Web クライアントは明示的にその要求を直接 Content Engine に送信するように設定しておく）があります。

（注）　Setup ユーティリティはスタンドアロン Content Engine が起動するプロセス、および一般的に使用されるキャッシング サービス（表 4-2 を参照）を実行するプロセスを促進します。

ACNS ネットワーク デバイスのタイプ

表 1-1 では、3 つの異なるタイプの ACNS ネットワーク デバイスを示しています。

表 1-1　ACNS ネットワーク デバイスのタイプ

デバイス	説明	詳細
Content Distribution Manager	ACNS 5.x ネットワーク デバイス（Content Distribution Manager に登録された Content Router、Content Engine）の設定と監視、コンテンツの獲得と配信、およびサービスを含む中央化されたコンテンツとデバイスの管理ステーションです。個別に管理するのではなく、グループとして中央でデバイス（Content Engine および Content Router）を管理できます。	『中央管理配置に関する Cisco ACNS ソフトウェア コンフィギュレーション ガイド Release 5.3』を参照してください。
Content Engine	要求されたコンテンツをクライアントに供給します。Content Engine を配置するには、次の 2 つの方法があります。 • スタンドアロン Content Engine（このマニュアルで説明しています） または • Content Distribution Manager に登録された Content Engine（『中央管理配置に関する Cisco ACNS ソフトウェア コンフィギュレーション ガイド Release 5.3』を参照してください）	スタンドアロン Content Engine の概要については、「スタンドアロンの Content Engine について」（P. 1-5）を参照してください。
Content Router	コンテンツ要求をクライアントに最も近くにある、登録されている Content Engine にリダイレクトする。このタイプの要求リダイレクションはコンテンツ ルーティングと呼ばれます。コンテンツ ルーティングに関して、Content Engine は Content Distribution Manager に登録されていなければなりません。スタンドアロン Content Engine はコンテンツ ルーティングをサポートしません。	『中央管理配置に関する Cisco ACNS ソフトウェア コンフィギュレーション ガイド Release 5.3』を参照してください。

（注）　ACNS ソフトウェアのデバイス モードで、ACNS デバイスが Content Distribution Manager、Content Engine、または Content Router のいずれかとして機能するかを設定します。**device mode** グローバル設定コマンドを介して、デバイス モードを指定できます。デフォルトのデバイス モードは、Content Engine です。

次の配置例が示すように、ACNS 5.x ネットワークが機能するために、3 タイプの ACNS ネットワーク デバイスすべてが存在する必要はありません。

- 配置 A：単一スタンドアロン Content Engine（Content Distribution Manager および Content Router のない）
- 配置 B：複数のスタンドアロン Content Engine（Content Distribution Manager および Content Router のない）
- 配置 C：1 台の Content Distribution Manager および複数の Content Engine（Content Distribution Manager に登録されている）があり、Content Router はない
- 配置 D：1 台の Content Distribution Manager 、複数の Content Engine（Content Distribution Manager に登録されている）、および 1 台または複数の Content Router がある

スタンドアロンの Content Engine について

Content Engine は ローカル ネットワーク上のエンド ユーザ（Web クライアント）の近くにある Content Engine にコンテンツを保存し、配信することにより、すべての HTTP で配信可能なストリーミング メディア形式のコンテンツを高速化します。「Web クライアント」という用語は、ブラウザまたはメディア プレーヤーを使用してコンテンツや情報を要求するエンド ユーザを意味します 。サポートされている Web クライアントの詳細は、「スタンドアロン Content Engine がサポートしている Web クライアント」（P. 1-14）を参照してください。

Content Engine を配置するには、次の 2 つの方法があります。

- インターネット ネットワーク上のファイアウォールの内側に配置する。
- 企業ネットワークのエッジ（営業所）に配置する。

（注）　スタンドアロン Content Engine を複数配置できます（たとえば、スタンドアロン Content Engine クラスタ構成で配置することもできます）。

スタンドアロン Content Engine は、次のタイプのクライアントからのコンテンツ要求を処理します。

- Web ブラウザ（たとえば、Microsoft Internet Explorer）
- ストリーミング メディア プレーヤー（たとえば、Windows Media Player、RealMedia Player [RealPlayer および RealOne Player]）。

コンテンツに対するクライアント要求は、次の 1 つまたはそれ以上の方法でスタンドアロン Content Engine にルーティングされます。

- 要求を直接非透過フォワード プロキシ サーバとして動作する Content Engine に送信するようにクライアント ブラウザとメディア プレーヤーを設定する直接プロキシ ルーティング
- 透過リダイレクト（ルータとスイッチは透過的に Web 要求を代行受信し、検査と操作を行うためにその要求を Content Engine に送信する）
  - WCCP ルーティング
  - レイヤ 4 スイッチ

  透過リダイレクトを使用して、WCCP 対応ルータまたはレイヤ 4 スイッチは透過的にクライアント要求を代行受信し、その要求を目的のサーバではなく、Content Engine にリダイレクトします。Content Engine は、目的のサーバのように機能し、要求に応答し、クライアントとの接続を確立します。実際には Content Engine と接続していても、ライアントは目的のサーバと接続が確立したとみなします。透過リダイレクトの詳細は、「透過モードでのキャッシングおよびストリーミング サービスの配置」（P. 3-8）を参照してください。

単一の環境で、1 つ以上のルーティング方式を使用することができます。たとえば、スタンドアロン Content Engine を設定して、HTTP、FTP-over-HTTP 要求を処理する直接プロキシ ルーティングを使用できますが、Windows Media Technologies（WMT）の要求には、透過リダイレクトを使用することができます。コンテンツ要求をスタンドアロン Content Engine にルーティングするために使用されるルーティング方式は、Content Engine がサポートできるコンテンツ サービスのタイプを判別します。詳細は、「スタンドアロン Content Engine を使用するキャッシングとストリーミング サービス」（P. 1-10）を参照してください。

（注）　コンテンツ ルーティングは、スタンドアロン Content Engine ではサポートされません。コンテンツ ルーティングを使用する場合は、Content Distribution Manager に Content Engine を登録する必要があります。コンテンツ ルーティングに関する情報は、『中央管理配置に関する Cisco ACNS ソフトウェア コンフィギュレーション ガイド Release 5.3』を参照してください。

ACNS ネットワークで配信されるコンテンツ タイプ

コンテンツは、ACNS ネットワーク上の基本要素であり、ACNS ネットワークが処理するデータのすべてを表します。コンテンツは、ファイルまたはメディア ストリームの形であり、オンデマンド、事前ロード、事前配信、またはライブに分類されます。コンテンツは、その獲得、配信、またはサービスの方法に基づいて分類されます。

表 1-2 では、ACNS 5.x ネットワークで配信できる各種のコンテンツ タイプを説明します。

（注）　事前配信されるコンテンツは Content Distribution Manager に登録されている Content Engine でのみサポートされます。事前配信されるコンテンツは、スタンドアロン Content Engine ではサポートされませんが、事前ロード コンテンツはスタンドアロン Content Engine でサポートされます。

表 1-2　ACNS ネットワークで配信されるコンテンツ タイプ

コンテンツのタイプ Content Engine	説明
オンデマンド	ユーザ要求（クライアントがトリガーしたデマンド）が原因で獲得され、キャッシュされ、そして配信されるコンテンツ（図 1-1 を参照）。このタイプのキャッシングはデマンド プル キャッシングと呼ばれます。スタンドアロン Content Engine が透過モード（Content Engine が透過リダイレクトで要求を受信する）で動作している場合、または非透過モード（Content Engine が Web クライアントから直接要求を受信する）で動作している場合、スタンドアロン Content Engine 上でデマンドプル キャッシングを設定できます。 HTTP を通してして取得されるキャッシュ コンテンツは、Content Engine 上のキャッシュ ファイル システム（cfs）のストレージ区画に保存されます。2 つのストリーミング プロトコル（WMT と RTSP）を通してして取得されるキャッシュ コンテンツは、Content Engine 上のメディア ファイル システム（mediafs）のストレージ区画に保存されます。
事前ロード	ユーザのコンテンツ要求を予測して特定のコンテンツの取得をスケジュールすることにより、取得され、スタンドアロン Content Engine に保存されたコンテンツ。次のタイプのコンテンツは、スタンドアロン Content Engine に事前ロードされます。HTTP URL、FTP-over-HTTP URL、および MMS URL（WMT ストリーミング メディア ファイル）。設定済みのすべての HTTP、FTP-over-HTTP、および MMS のパラメータとルールが、事前ロードされるオブジェクトに適用されます。事前ロード プロセス時に、スタンドアロン Content Engine は、コンテンツを取得するために、Web サイトのリンク レベルをスキャンし、特定のコンテンツを取得し、ローカルに保存します。Content Engine がこのコンテンツ要求を受信すると、Content Engine はコンテンツをローカル ストレージから配信します。これにより、WAN 帯域幅を節約し、さらに Web クライアントへのコンテンツ配信を高速化できます。 Content Engine の事前ローデング コンテンツの詳細については、「スタンドアロン Content Engine のコンテンツ事前ローディングの設定」（P. 11-2）を参照してください。

表 1-2　ACNS ネットワークで配信されるコンテンツ タイプ（続き）

コンテンツのタイプ Content Engine	説明
事前配信	ACNS ネットワーク管理者がユーザの要求を予測して、これらの Content Engine 上のコンテンツの獲得と配信を設定することにより、Content Distribution Manager に登録されている Content Engine のネットワークを介して、取得および配信されるコンテンツ。 このコンテンツは、中央で管理された ACNS ネットワーク環境で、Content Engine に保存されるコンテンツを配信する手段として使用されます。帯域帯を消費するコンテンツ オブジェクト（たとえば、Java アプレット、Macromedia Flash アニメーション、Shockwave プログラムやその他のファイル形式）は、オフピーク時に Content Engine に配信されるように管理され、スケジュールされます。 事前配信コンテンツの管理に関する情報については、『中央管理配置に関する Cisco ACNS ソフトウェア コンフィギュレーション ガイド Release 5.3』を参照してください。
ライブ	オリジン サーバからブロードキャストされるコンテンツ ストリーム（一般的には、ストリーミング メディア。このコンテンツは、衛星または地上のどちらかのブロードキャスティング ソースからライブ ストリーミング ブロードキャストとして獲得されます。）ライブ マルチメディア ストリームの取得に関連したポリシー（たとえば、プログラム リスト URL（再生リスト）、最大ビット レートなど）、および配信ポリシー（たとえば、優先順位、スケジュール、最大帯域幅）を設定します。 WMT ライブ ストリームを配信するスタンドアロン Content Engine の設定方法については、「WMT ライブ ストリームを配信するためのスタンドアロン Content Engine の設定」（P. 9-51）を参照してください。

この章の後半では、スタンドアロン Content Engine の配置についてのみ説明します。Content Engine がサポートしているルーティング方式およびコンテンツ サービスは、Content Engine がスタンドアロンで稼働しているか、Content Distribution Manager に登録されているかにより異なります。Content Distribution Manager に登録されている Content Engine については、『中央管理配置に関する Cisco ACNS ソフトウェア コンフィギュレーション ガイド Release 5.3』を参照してください。

スタンドアロン Content Engine の機能概要

ここでは、スタンドアロン Content Engine の配置の概要について説明します。また構成は次のとおりです。

配置例のシナリオは、第 3 章「スタンドアロン Content Engine の配置シナリオ」を参照してください。

スタンドアロン Content Engine を使用するプロキシ サービス

スタンドアロン Content Engine は、次に示す重要なプロキシ サービスを提供するプロキシ サーバとして配置されます。

- フォワード プロキシ キャッシング
- リバース プロキシ キャッシング

（注）　プロキシ　サーバは、クライアントからのコンテンツ要求を受け入れる仲介者の役割を担うサーバです。プロキシ サーバがすでに要求されたコンテンツのコピーをローカル ストレージ（キャッシュ）に保存している場合、プロキシ サーバは要求に応じて、ローカル ストレージからコンテンツを配信します。それ以外は、オリジン サーバ、または他のプロキシ サーバに要求を転送します。プロキシ サーバは、クライアントおよびサーバの両方として機能します。コンテンツを要求している Web クライアントに対してはサーバとして動作します。また接続先のサーバ（たとえば、オリジン サーバまたは他のプロキシ サーバ［たとえば、指定された 上流の プロキシ サーバ］）にはクライアントとして動作します。プロキシ サーバは一般に、「プロキシ」と呼ばれています 。

フォワード プロキシ キャッシング

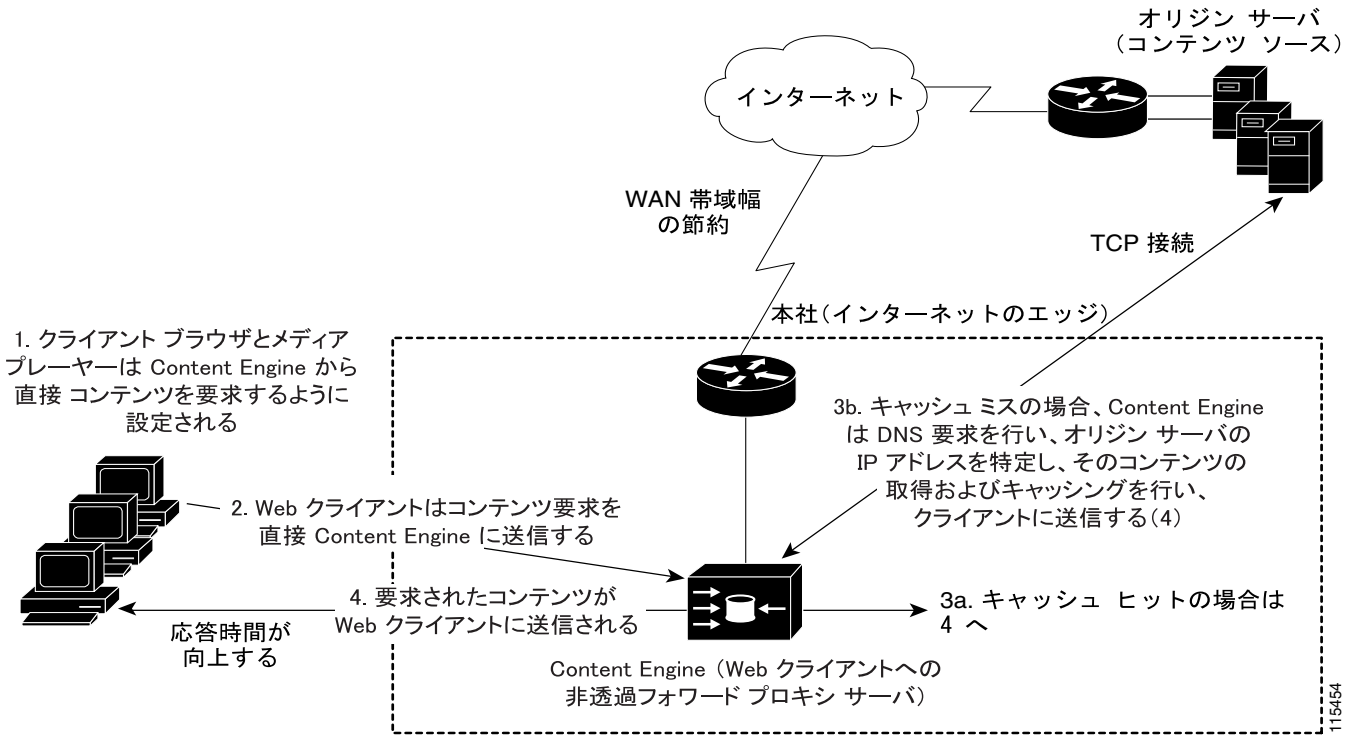
フォワード プロキシ キャッシングを使用すると、スタンドアロン Content Engine は Web クライアントに対して、プロキシ サーバとして動作します。Content Engine（フォワード プロキシ サーバ）は内部クライアントがファイアウォール経由でインターネットにアクセスできるようにします。

クライアント ブラウザおよびメディア プレーヤーが Content Engine（フォワード プロキシ サーバ）にコンテンツ要求を明示的に送るように設定されている場合、これを直接プロキシ ルーティングと言います 。クライアント要求を Content Engine に宛先を指示するために直接プロキシ ルーティングが使用されるとき、Content Engine は非透過モードで動作しています。クライアントは彼らの要求が Content Engine に宛先を指示されていることを知っています。Content Engine は特定のポリシーとルールを使用して、クライアントが要求したインターネット コンテンツへのアクセスを受け入れるか、拒否するかを判断します。このタイプのフォワード プロキシ サービスは通常、企業環境において大規模なインターネット セキュリティ ソリューションの一部として提供されます。このサービスを実行することにより、エンド ユーザ（Web クライアント）がファイアウォールの外にいたとしても、企業はそのプライベート ネットワークの完全性を脅かされることがなくなります。

直接プロキシ ルーティング方式は、最も簡単なルーティング方式です。このルーティング方式は一般的に、ユーザのデスクトップがしっかり管理されている場合に使用されます。そのため、直接プロキシ ルーティングはサービス プロバイダー環境ではなく、一般に企業環境で使用されます。クライアント要求を Content Engine に送信するために直接プロキシ ルーティングを使用する場合のフォワード プロキシ キャッシングの配置例については、図 1-2 を参照してください。クライアント

要求を Content Engine に送信するために直接プロキシ ルーティングを使用する場合にサポートされるキャッシングとストリーミング サービスのリストについては、表 1-5 を参照してください。直接プロキシ ルーティングを使用して、キャッシングとストリーミング サービスを運用する方法の詳細は、「非透過モードでのキャッシングおよびストリーミング サービスの配置」（P. 3-4）を参照してください。

図 1-2　直接プロキシルーティングを使用するフォワード プロキシ キャッシングの運用例



直接プロキシ ルーティングと同じ利点をもつ Content Engine を透過フォワード プロキシ サーバとして配置できますが、クライアント デスクトップの設定を変更する必要はありません。このタイプの配置では、クライアントはそのコンテンツ要求が Content Engine（透過フォワード プロキシ サーバ）にリダイレクトされていることを知りません。透過リダイレクト方式は、WCCP 対応ルータまたはレイヤ 4 スイッチ経由で実現できます。

透過リダイレクト方式では、ネットワーク トポロジおよびトラフィック パターンの理解を要求されますが、一般に組織はこの方式を好みます。これはいかなるクライアント デスクトップの設定を変更する必要がないからです。ただし、直接プロキシ ルーティングを使用するには、従来からの要件があります。また組織が特定のサービスに対して、直接プロキシ ルーティングを使用する必要がある場合（たとえば、HTTPS プロキシ キャッシングなど）もあります。これは営業所の WCCP 対応ルータまたはスイッチの設定を変更できないからです。詳細は、「透過リバース プロキシ キャッシングの概要」（P. 3-12）を参照してください。

リバース プロキシ キャッシング

リバース プロキシ キャッシングを使用すると、スタンドアロン Content Engine は Web サーバ ファーム内のサーバにはプロキシ サーバとして動作します。また Web クライアントはその HTTP 要求が透過的に Content Engine（透過リバース プロキシ サーバ）にリダイレクトされていることを知りません。このような配置では、Content Engine は Web サーバ ファーム内のサーバには プロキシとして動作します。

（注）　リバース プロキシ キャッシングとフォワード プロキシ キャッシングとの大きな違いは、リバース プロキシ キャッシングを使用すると、Content Engine は特定のコンテンツのみ（たとえば、Web サーバ ファーム内の Web サーバからのコンテンツのみ）をキャッシュするように設定されます。フォワード プロキシ キャッシングでは、Content Engine は可能なときはいつでも、コンテンツをキャッシュするように設定されます。

またリバース プロキシ キャッシングでは、ファイアウォール経由による内部コンテンツ（たとえば、会社のイントラネット上のコンテンツなど）に対する外部クライアントのアクセスを、スタンドアロン Content Engine が提供することを可能にします。一般に、このリバース プロキシ キャッシングは、セキュアな Web 公開をするために使用されます。リバース プロキシ キャッシュ設定では、プロキシ サーバはインターネット上でルーティング可能な IP アドレスを使用して設定します。Web クライアントは、ドメイン名の DNS 解決に基づいて、プロキシ サーバに対する宛先を指示されます。リバース プロキシ サーバは、クライアントからはオリジン Web サーバのように見えます。

スタンドアロン Content Engine にリバース プロキシ キャッシングを配備するいくつかの重要な利点は、次のとおりです。

- サーバ ファームからスタティック イメージの処理の負担を軽減することで、Web サーバの拡張の代替方法を提供する。リバース プロキシ サーバにコンテンツ着信要求を透過的に処理させることにより、Web トラフィックは大幅に削減します。
- Content Engine　を地理的に分散した地域に配置して、これらの区域にコンテンツを複製することができる。
- クライアントの設定を変更する必要がまったくない（クライアント　ブラウザを設定して、リバース プロキシ サーバとして機能している Content Engine を指定する必要がない）。

リバース プロキシ キャッシングは、WCCP サービス（サービス 99）です。そのため、ルータと Content Engine は両方ともリバース プロキシ サービスを実行するように設定する必要があります。クライアント要求を Content Engine に送信するために透過リダイレクトを使用する場合にサポートされるキャッシングとストリーミング サービスのリストについては、表 1-6 を参照してください。リバース プロキシ キャッシング サービスを運用する方法の詳細は、「透過リバース プロキシ キャッシングの概要」（P. 3-12）を参照してください。

スタンドアロン Content Engine を使用するキャッシングとストリーミング サービス

ACNS ソフトウェアは、各種のキャッシングとストリーミング メディア サービスをサポートしています。スタンドアロン Content Engine 上で設定できるサービスのタイプは、コンテンツ要求が Content Engine に対してどのようにルーティングされるかにより異なります。

表 1-3 では、ACNS 5.x ソフトウェアがサポートするストリーミング メディア ソリューション（Microsoft の Windows Media Technologies（WMT）ソリューション、および RealNetworks, Inc.、Apple Computer と Cisco Systems, Inc. の Real-Time Streaming Protocol（RTSP）ソリューション）を示しています。

表 1-3　ACNS 5.x ソフトウェア ストリーミング メディア ソリューション

ソリューション	ソリューションの説明	スタンドアロン Content Engine	Content Distribution Manager に登録されている Content Engine
Microsoft WMT	ストリーミング メディアに対する Microsoft ソリューション。Microsoft 独自の Microsoft Media Server（MMS）プロトコルを使用します。 Windows Media Server 9（WMS 9）はまた RTSP/RTP プロトコル（IETF 標準の RTSP プロトコルに独自の拡張を加えたもの）もサポートします。ACNS 5.3 ソフトウェア リリースでは、WMS 9-over-RTSP のサポートが追加されました。	WMT プロキシおよびサーバが、Content Engine にインストールされます。Windows Media クライアントはストリーミング メディア コンテンツを要求します。	スタンドアロン Content Engine と同じ。
RealNetworks RealMedia	ストリーミング メディアに対する RealNetworks, Inc. ソリューション。RealNetworks RTSP プロトコル（IETF 標準の RTSP プロトコルに独自拡張機能を追加）を使用します。	RealProxy は、インストール可能な、唯一の RealMedia コンポーネントです。RealProxy は、RealNetworks RTSP プロトコルを使用して、RealMedia クライアント（RealPlayer および RealOne Player）にコンテンツを配信します。	すべてのRealMedia コンポーネント（たとえば、RealProxy と RealSubscriber など）を Content Engine 上にインストールできることを除いて、スタンドアロン Content Engine と同じです。これは Content Engine が Content Distribution Manager に登録されているからです。
Apple QuickTime	IETF 標準の RTSP プロトコルを使用するストリーミング メディアに対する Apple Computer ソリューション。	サポート対象外。	Cisco Streaming Engine が Content Engine 上で動作し、QuickTime 準拠のコンテンツ（たとえば、MOV および MPEG-1 コンテンツ）を QuickTime クライアントに配信します。
Cisco Streaming Engine	IETF 標準の RTSP プロトコルを使用する Cisco RTSP ベースのストリーミング メディア ソリューション。	サポート対象外。	Cisco Streaming Engine は、Content Engine 上で動作し、事前配信コンテンツを配信します。 またローカル ユーザに配信する、ライブ ストリーミング サービスとビデオ オン デマンド（VOD）ストリーミング サービスに対する IP/TV 統合機能をサポートするためにも使用されます。

（注）　クライアント要求をスタンドアロン Content Engine に送信するために、直接プロキシ ルーティングまたは透過リダイレクトを使用する場合にサポートされるキャッシングとストリーミング サービスのリストについては、表 1-5 および 表 1-6 を参照してください。

RTSP は、標準のインターネット ストリーミング制御プロトコル（RFC2326）です。RTSP は、アプリケーション レベルのプロトコルで、リアルタイム性をもつビデオやオーディオなどのストリーミング メディアの配信を制御します。また、このプロトコルは、キャッシングおよび ACNS 環境でのストリーミングメディア プロトコルとして広く普及しています。Apple QuickTime、RealNetworks RealProxy、および Cisco Streaming Engine はすべて、ストリーミング メディア プロトコルとして RTSP を使用するバックエンド RTSP サーバです。スタンドアロン Content Engine 上では、RealProxy のみがサポートされています。

RealNetworks RealProxy の機能は、RealNetworks RTSP プロトコルを使用しています。これには、IETF 標準の RTSP プロトコルに RealNetworks 独自の拡張機能が組み込まれています。RealProxy の機能を使用すると、スタンドアロン Content Engine は RealMedia 透過プロキシ キャッシングをサポートできます。また RealProxy を使用すると、Content Engine はキャッシュされた VOD ファイルを RealMedia Player に流すこと、およびストリーミングし、ライブ分割をサポートすることが可能になります。

RealProxy の機能は、ライセンスを受けた RealNetworks ソフトウェアです。この機能を Content Engine 上で有効にするには、RealProxy ライセンス キーを取得する必要があります。このキーは Content Engine に付属する証明書に表示されています。ACNS 5.x ソフトウェアをダウンロードして利用する場合は、Cisco.com Web サイトから RealProxy ライセンスを購入できます。詳細は、「RealMedia サービスの設定」（P. 8-10）を参照してください。スタンドアロン Content Engine の RTSP ストリーミング メディア サービスの詳細は、第 8 章「スタンドアロン Content Engine の RealMedia サービスの設定」を参照してください。

Cisco Streaming Engine を使用して、RTSP ベースのコンテンツを Content Distribution Manager に登録されている Content Engine に事前配信できます。Cisco Streaming Engine は標準 RTSP プロトコルを使用して、QuickTime 準拠のコンテンツ（たとえば、MOV および MPEG-1 コンテンツなど）をクライアントに配信します。

Cisco IP/TV は、Cisco コンテンツ ネットワーキング製品ファミリーのメンバーです。Cisco IP/TV の構成は、IP/TV Program Manager、1 台またはそれ以上の IP/TV Broadcast Server、および IP/TV Viewer または QuickTime Web プラグインです。IP/TV ネットワークの中央管理プラットフォームである、IP/TV Program Manager は、レコーディング機能だけでなく、ライブ イベントと再ブロードキャスト イベントおよび VOD ファイルのスケジュールを作成したり、ポリシーを設定するためのシンプルなインターフェイスを提供します。IP/TV Broadcast Server は、リアルタイム エンコーディング、およびライブ ビデオ、スケジュールされたビデオ、およびオンデマンド ビデオの配信を提供します。

Cisco Streaming Engine を IP/TV リリース 5.1 ソフトウェア、またはそれ以降と組み合わせて使用すると、ライブ ストリーミング サービスと VOD ストリーミング サービスの両方をローカル ユーザに配信できます。次の 2 つの例では、Cisco IP/TV ソリューション（IP/TV リリース 5.1 またはそれ以降）を ACNS 5.1 ソフトウェアとそれ以降、および Content Distribution Manager に登録された Content Engine と一緒に使用する方法を示しています。

- IP/TV を使用して作成されるライブ イベントをレコードして、そのコンテンツを ACNS 5.1 ソフトウェアまたはそれ以降を使用して配信する。
- IP/TV ライブ イベントの範囲を拡張するか、または「マルチキャスト アイランド」に、ACNS 5.1 ソフトウェアまたはそれ以降を介してイベントを再ブロードキャストする。「マルチキャスト アイランド」という用語は、ユニキャスト WLAN および マルチキャスト LAN を組み合わせた、非マルチキャスト対応のネットワークまたは環境のことを指します。

  ACNS 5.1 ソフトウェアでは、4 番目のデバイス モード（Program Manager）が追加され、特定のデバイスを使用して、IP/TV と ACNS ソフトウェア ネットワーク（リリース 5.1 およびそれ以降）との統合をサポートできるようになりました。たとえば、Program Manager をデバイス モードとして指定することにより、Content Engine CE-565 または CE-7305 モデルを IP/TV Program Manager として設定できます。デバイス モードの変更をサポートするデバイス上で、

Setup ユーティリティを起動すると、デバイス モードを指定するように要求されます。Setup ユーティリティを使用して、デバイスを Program Manager として設定するには、デバイス モードとして、**PM** を次のように指定します。

```
What is the mode of the device (CE/CR/CDM/PM) [CE]: PM
```

Cisco IP/TV および Cisco Streaming Engine は、スタンドアロン Content Engine 上ではサポートされません。Cisco Streaming Engine の配置に関する情報は、『中央管理配置に関する Cisco ACNS ソフトウェア コンフィギュレーション ガイド Release 5.3』を参照してください。Cisco IP/TV の詳細情報は、Cisco IP/TV 5.x 製品のマニュアルを参照してください。

キャッシングとストリーミングでサポートされているプロトコル

Web クライアント（ブラウザまたはメディア プレーヤー）と Web サーバとの対話は、HTTP、MMS、および RTSP などの既存の標準アプリケーション レイヤで動作するインターネット プロトコルを使用します。Content Engine は、これらのすべての Web アクセス プロトコルを使用して、Web オブジェクトを Web クライアントに配信できる必要があります。

表 B-1 では、ACNS 5.3.x ソフトウェアを実行している Content Engine が Web クライアントにコンテンツを配信するために使用する、ネットワーク プロトコルについて説明しています。表 B-2 では、スタンドアロン Content Engine を使用して、ストリーミング メディア ファイルを配信するために使用できるストリーミング メディア プロトコル、制御チャネル、対応するデータ形式、および伝送タイプをリストしています。

HTTP、FTP、TFTP、HTTPS および IETF 標準 RTP/RTSP プロトコルのサポートは、（ACNS 5.1 ソフトウェアまたはそれ以降）の一部として組み込まれています。以下の 2 つの機能に関するサポートには別々のライセンスが必要です。

- Microsoft 独自の MMS プロトコルを使用する WMT の機能には WMT のライセンスが必要です。詳細は、「スタンドアロン Content Engine 上の WMT RTSP ストリーミングおよびキャッシング サービスの設定」（P. 9-21）を参照してください。
- IETF 標準の RTSP プロトコルに独自の拡張を組み込んだ、RealNetworks の RTSP プロトコルを使用する RealNetworks RealProxy の機能には RealProxy のライセンスが必要です。詳細は、「RealMedia サービスの設定」（P. 8-10）を参照してください。

スタンドアロン Content Engine がサポートしている Web クライアント

表 1-4 では、ACNS 5.3.x ソフトウェアを実行している、スタンドアロン Content Engine と通信できる Web クライアントをリストしています。

表 1-4　スタンドアロン Content Engine がサポートしている Web クライアント

クライアント プロトコル	クライアント
HTTP プロトコル • HTTP • HTTPS-over-HTTP • MMS-over-HTTP	Microsoft Internet Explorer、Netscape などを含む HTTP 1.0 または HTTP 1.1 の仕様に準拠する すべてのインターネット ブラウザ。 Windows Media Player（バージョン 6.x および 7.x）は、Content Engine からコンテンツを要求するために、MMS-over-HTTP を使用することができます。
FTP-over-HTTP	FTP 要求を出すクライアント ブラウザ（ACNS 5.1 ソフトウェア リリースでサポートが追加されました）。
ネイティブ FTP	クライアントからの FTP ネイティブな要求に対して、非透過プロキシ サーバとして動作する Content Engine に向けて、FTP ネイティブな要求を出す FTP クライアント（たとえば、Reflection X クライアント、WS-FTP クライアント、または Unix あるいは DOS コマンドライン FTP プログラム）（ACNS 5.3.1 ソフトウェア リリースでサポートが追加されました）。
Trivial File Transfer Protocol（TFTP）	TFTP クライアント（ACNS 5.1 ソフトウェア リリースでサポートが追加されました）。
RealNetworks 専用 RTSP プロトコル	Real Media Player は Content Engine からコンテンツを要求するためにこのプロトコル（IETF 標準の RTSP プロトコルに RealNetworks 独自の拡張を加えたもの）を使用します。 以下のメディア プレーヤーをまとめて RealMedia Player といいます。 • RealNetworks, Inc. の RealPlayer（Version 8.x およびそれ以降） • RealOne プレーヤー
Microsoft 独自の RTSP プロトコル	WIndows Media 9 Player は Content Engine からコンテンツを要求するために、TCP モードでこのプロトコル（IETF 標準の RTSP プロトコルに Microsoft 独自の拡張を加えたもの）を使用します（ACNS 5.3.1 ソフトウェア リリースでサポートが追加されました）。
MMS プロトコル • MMS-over-TCP（MMST） • MMS-over UDP（MMSU）	以下のメディア プレーヤーをまとめて WMT プレーヤーといいます。 • Microsoft の Windows Media Player（Version 6.x およびそれ以降） • Microsoft の Windows Media Series 9 Player（ACNS 5.2 ソフトウェア リリースで追加されました）

スタンドアロン Content Engine はライブ コンテンツまたは、オンデマンド コンテンツとしてストリーミング メディア（たとえば、VOD ファイルなど）を RealMedia Player および WMT Player に配信できます。スタンドアロン Content Engine は QuickTime Player または、Cisco IP/TV Viewer からの要求をサポートしません。

直接プロキシ ルーティングを使用してサポートされるキャッシングとストリーミング サービス

表 1-5 では、直接プロキシ ルーティングを使用して、クライアント要求をスタンドアロン Content Engine に送信する場合にサポートされるキャッシングとストリーミング サービスについて示しています。アスタリスク（*）は、特定のキャッシング サービスは Content Engine CLI を使用する以外にも Setup ユーティリティを使用して設定できることを示しています。

表 1-5　直接プロキシ ルーティングを使用してキャッシングとストリーミング サービス

Services	詳細
従来のキャッシング	
HTTP フォワード プロキシ キャッシング *	スタンドアロン Content Engine における非透過 HTTP フォワード プロキシ キャッシングの設定
FTP-over-HTTP キャッシング	スタンドアロン Content Engine における非透過 FTP-over-HTTP キャッシングの設定
FTP ネイティブ キャッシング	非透過 FTP ネイティブ キャッシングの設定
HTTPS プロキシ キャッシング	スタンドアロン Content Engine における HTTPS キャッシングの設定
WMT キャッシングとストリーミング	
WMT プロキシ キャッシング *	スタンドアロン Content Engine 上での WMT キャッシングの有効化と設定
ライブ WMT ストリーミングのストリーミング	WMT ライブ ストリームを配信するためのスタンドアロン Content Engine の設定
事前ロードされた VOD ファイルのストリーミング	VOD ファイルを配信するスタンドアロン Content Engine の設定
RTSP キャッシングとストリーミング	
RealMedia プロキシ キャッシング *	直接プロキシ ルーティングおよび RealMedia プロキシ キャッシングの設定
キャッシュされた VOD ファイルとライブ分割の RealProxy ストリーミング VOD ファイルのキャッシング	RealMedia サービスの設定

透過リダイレクトを使用して、サポートされるキャッシングとストリーミング サービス

表 1-6 では、Content Engine が透過リダイレクトを使用して要求を受信する場合にサポートされる、キャッシングとストリーミング サービスを示します。アスタリスク（*）は、特定のキャッシング サービスは Content Engine CLI を使用する以外にも Setup ユーティリティを使用して設定できることを示しています。

表 1-6　透過リダイレクトを使用するキャッシングとストリーミング サービス

Services	詳細
従来のキャッシング	
HTTP リバース プロキシ キャッシング*	スタンドアロン Content Engine における HTTP リバース プロキシ キャッシングの設定
FTP ネイティブ キャッシング	透過 FTP ネイティブ キャッシングの設定
HTTPS 透過キャッシング	スタンドアロン Content Engine における HTTPS 透過キャッシングの設定
HTTP 透過キャッシング *	スタンドアロン Content Engine における透過 HTTP フォワード プロキシ キャッシングの設定
DNS キャッシング	DNS キャッシング ネーム サービス（サービス 53）用の DNS サーバの設定
WMT キャッシングとストリーミング	
WMT 透過キャッシング *	スタンドアロン Content Engine 上での WMT キャッシングの有効化と設定
WMT ライブ ストリーミングのストリーミング	WMT ライブ ストリームを配信するためのスタンドアロン Content Engine の設定
事前ロードされた VOD ファイルのストリーミング	VOD ファイルを配信するスタンドアロン Content Engine の設定
RTSP キャッシングとストリーミング	
RealMedia 透過 キャッシング*	RTSP 透過リダイレクションおよび RealMedia 要求のキャッシングの設定
キャッシュされた VOD ファイルとライブ分割の RealProxy ストリーミング	RealMedia サービスの設定

（注）　RealProxy は、Content Engine CLI または Setup ユーティリティを使用して、有効になります。RealProxy は、デフォルトの設定ファイルを使用して、有効になります。RealProxy のデフォルトの設定を変更するには、RealNetworks RealSystem Administrator GUI を使用する必要があります。RealProxy のデフォルト設定ファイルを元に戻すには、スタンドアロン Content Engine 上で Content Engine CLI を使用して、**rtsp real-proxy default-configuration** EXEC コマンドを入力します。詳細については、「RealMedia サービスの設定」（P. 8-10）を参照してください。

スタンドアロン Content Engine を使用したフィルタリングとアクセス コントロール

スタンドアロン Content Engine の他の重要な機能は、Web コンテンツに対して、フィルタリングとアクセス コントロールを行うことです。Content Engine を設定して、そのローカル データベースまたは遠隔地の AAA（Authentication, Authorization, and Accounting; 認証、許可、アカウンティング）サーバを使用して、クライアント要求を認証し、許可することができます。ACNS ソフトウェア 5.2.1 またはそれ以降を使用すると、TACACS+ 経由で AAA アカウンティングも使用できます（第 18 章「スタンドアロン Content Engine での AAA アカウンティングの設定」を参照）。

URL フィルタリングおよび Rules Template を使用して、URL へのアクセスをブロックする、または実際のコンテンツ ストリーム（たとえば、特定のヘッダーの書き換えなど）を変更することができます。アクセス コントロール リスト（ACL）を使用すると、特定のアドレス、アドレスのグループ、またはユーザ グループにフィルタを適用することができます。これらのポリシーに加え、帯域幅制限、およびクライアント要求を本当に受け入れるのかどうかを判別するリソース制御があります。

（注）　スタンドアロン Content Engine 上でサポートされているアクセス コントロールおよびフィルタリング サービスは、コンテンツ プロトコル（たとえば、アクセス コントロールは HTTP、HTTPS、および FTP-over-HTTP 要求をサポートしており、ICAP は HTTP および FTP-over-HTTP 要求のみをサポートしています）によって異なります。ACNS 5.3.x ソフトウェアを実行しているスタンドアロン Content Engine でサポートされているアクセス コントロールおよびフィルタリング コンテンツ サービスのリストについては、表 B-5 を参照してください。

ACNS 5.2.3 ソフトウェア以降では、一定の信頼できる HTTP および HTTPS 要求に対する URL フィルタリングをバイパスするように、Content Engine を設定することもできます。この機能に関する詳細情報は、「特定の HTTP および HTTPS 要求に対して URL フィルタリングをバイパスする Content Engine の設定」（P. 11-39）を参照してください。

スタンドアロン Content Engine は、コンテンツに対するクライアントの要求を受け取ると次のタスクを実行します。

- Web　クライアントを認証し、ユーザ名とパスワードを入力するようにクライアントに要求して、AAA サーバに照会し、そのクライアントが、Web にアクセスする許可を得ているかどうかを確認する。このタイプの認証と許可をコンテンツ認証といいます。詳細情報は、「スタンドアロン Content Engine を使用した認証、許可、およびアカウンティング」（P. 1-18）を参照してください。
- 要求をフィルタ（Websense や SmartFilter など）に通し、要求されたオブジェクトが好ましくないコンテンツでないことを確認する。詳細情報は、第 11 章「スタンドアロン Content Engine 上でのコンテンツ事前ローディングと URL フィルタリングの設定」を参照してください。

（注）　ACNS 5.x ソフトウェアは、第三者ソフトウェアを使用して、コンテンツのフィルタリングを実行します。サポートされているフィルタリング ソフトウェアには、Websense、N2H2、および SmartFilter などがあります。

- コンテンツを設定済みのルールと照合し、特定のヘッダーの書き換え、要求の転送、またはその他の方法による要求の処理を行う。プロトコルごとにサポートされているルール アクションのリストについては、表 13-2 を参照してください。スタンドアロン Content Engine 上でルールを設定する方法については、第 13 章「スタンドアロン Content Engine の Rules Template の設定」を参照してください。

- 要求されたコンテンツがすでに Content Engine のキャッシュ内に存在しているかどうかを確認する。もし存在する場合、Content Engine は、オリジン サーバからではなく、ローカル キャッシュから直接オブジェクトを供給するので、インターネットに使用する帯域幅を節約します。
- 要求されたコンテンツがまだキャッシュ内にない場合、クライアントに代わって Contene Engine がインターネットからそのコンテンツを取得し、必要ならば以後の使用に備えてそのコンテンツをキャッシュする。ACNS 5.x ソフトウェアは、Web アクセス プロトコル（HTTP を含む）、および表 B-1 にリストするすべてのストリーミング プロトコルをサポートすることによりこの機能をサポートしています。

ACNS 5.1 ソフトウェアまたはそれ以降を実行しているスタンドアロン Content Engine は、IP パケット フィルタリングもサポートしています。IP パケット フィルタリングは、Content Engine 上の特定のインターフェイス（サービス）に対するアクセスを制御します。IP パケットが Content Engine 上の特定のインターフェイスを通過することを許可するかどうかを指定する、IP ACL を設定できます。たとえば、IP ACL を使用して、Content Engine 上のコンテンツ配信および管理サービスへのアクセスを制御できます。詳細については、第 19 章「スタンドアロン Content Engine での IP アクセス コントロール リストの作成と管理」を参照してください。

スタンドアロン Content Engine を使用した認証、許可、およびアカウンティング

ACNS 5.x ソフトウェアは、外部アクセス サーバ（たとえば、RADIUS または TACACS+ サーバ）を使用するユーザ、および AAA 機能を使用するローカル アクセスのデータベースを必要とするユーザに対して、認証（Authentication）、許可（Authorization）、アカウンティング（Accounting）（AAA）をサポートします。

- 認証（または「ログイン」）は、ユーザを識別するアクションです。ユーザ名とパスワードがチェックされます。
- 許可（または「設定」）は、ユーザは何をすることが許されているかを識別するアクションです。ネットワーク内で認証されたユーザに対する権限を許可または拒否します。たとえば、スーパーユーザ管理者アカウント（たとえば、事前に定義された管理者アカウント）を使用してスタンドアロン Content Engine にログインする場合、最高レベルのアクセス権限を持つことになり、次の管理タスクをすべて実行することが可能です。
  - スタンドアロン Content Engine を設定する。
  - スタンドアロン Content Engine が収集した統計情報を取得する。
  - デバイスをリブートする。

（注）　一般に、認証は許可に優先されます。認証は義務ではありません。

- アカウンティング は、システムのアカウンティングの目的で管理者ユーザのアクティビティを追跡するアクションです。ACNS 5.2.1 ソフトウェア以降では、TACACS+ を使用する AAA アカウンティングがサポートされています。詳細情報は、第 18 章「スタンドアロン Content Engine での AAA アカウンティングの設定」を参照してください。

ACNS 5.x 環境では、認証と許可という 2 つの主要なタイプがあります。

- コンテンツ認証：Content Engines により供給されるコンテンツに対するエンド ユーザ アクセスを制御する。このトピックに関する詳細情報は、第 10 章「スタンドアロン Content Engine のコンテンツ認証および許可の設定」を参照してください。
- 管理上のログイン認証：監視、設定、またはトラブルシューティングの目的で管理者が Content Engine にログオンするための要求を処理する、管理上のログイン認証方式（ローカル、RADIUS、TACACS+）を制御する。

管理者はコンソールまたは Content Engine GUI を使用して、スタンドアロン Content Engine にログインできます。これらの管理者ログイン要求を処理するために、Content Engine は指定された認証データベースをチェックし、ユーザのユーザ名とパスワードを確認し、この特別な管理者がこのログイン セッション時に承認されるアクセス権を判別します。Content Engine はログイン要求を受信すると、ローカル データベースまたは遠隔地のサードパーティ データベース（TACACS+ データベースまたは RADIUS データベース）をチェックし、ユーザ名とパスワードを確認し、管理者アクセス権を判別します。

これらの認証と許可の方式を任意に組み合わせて設定し、スタンドアロン Content Engine への管理ログイン アクセスをコントロールできます。

- ローカル認証および許可
- RADIUS
- TACACS+

デフォルトでは、Content Engine は、管理ログイン要求を処理する基本方式として、ローカル ログイン認証方式を使用します。ローカル認証を他の認証方式とともに有効にし、優先順位のフラグを設定していない場合、ローカル認証が常に実行されます。コンソールおよび Telnet 接続では、複数の異なる管理上のログイン認証方式を指定できません。詳細情報は、第 17 章「スタンドアロン Content Engine での管理ログイン認証と許可の設定」を参照してください。

（注）　コンテンツ認証と許可は、管理者ログイン認証と許可とは無関係です。

ACNS 5.3.x ソフトウェアを実行しているスタンドアロン Content Engine でサポートされているキャッシング、フィルタリング、および認証方式のリストについては、表 B-4 を参照してください。

スタンドアロン Content Engine を使用したモニタリング機能とトラブルシューティング機能

パフォーマンスを測定して、設定の調整に必要な兆候を見つけたり、Content Engine を追加導入したりするためには、Content Engine をモニタリングすることが重要です。ACNS 5.3 ソフトウェアを実行しているスタンドアロン Content Engine のパフォーマンスを監視するために各種のツールが用意されています。このツール セットは、Cisco Discovery Protocol（CDP）、Simple Network Management Protocol（SNMP）、ACNS ソフトウェア アラームから構成されています。このトピックに関する詳細は、「スタンドアロン Content Engine のモニタリング」（P. 21-2）を参照してください。

Content Engine のパフォーマンスを監視するだけでなく、トランザクションを監視する機能もサポートされています。

（注）　「トランザクション」という用語は、クライアントが完了した Web リソースに対する成功要求、または失敗要求のことを言います。ACNS 5.x ソフトウェアが実行されているスタンドアロン Content Engines では、レポートの目的で、すべてのエラーとアクセス アクティビティを記録できます。

ACNS 5.x ソフトウェアでは、Content Engines 上の各コンテンツ サービス モジュール（HTTP モジュール、WMT サーバ、FTP プロキシ プロセス、TFTP サーバなど）によって、サービスされた要求のログが記録されます。対応するロギングが用意されている要求には、HTTP 要求、HTTPS 要求、FTP 要求、WMT 要求、RTSP ストリーミング要求、および TFTP 要求があります。

各コンテンツ転送プロトコルには、対応する **show** *protocol-name* **statistics** EXEC コマンドがあり、そのプロトコルでの統計情報を表示します。

Content Engine の管理者は、一般的に、Content Engine 上で行われた要求のタイプや要求によってもたらされた結果に注目します。たとえば、ストリーミング メディアが会社の収入源である場合、その会社では、どのお客様がどのコンテンツにアクセスしたか、ユーザがどれくらいの時間コンテンツを見たか、また、その表示時の品質などをトラッキングする手段が必要になります。これらの会社では、オンデマンド コンテンツやライブ ブロードキャストの配信について課金する必要があるため、コンテンツ アクセス サービスに関するお客様への請求については、記録された情報に基づいて行う必要があります。

Content Engine がサービスする要求を記録するソフトウェア ログはトランザクション ログと呼ばれます 。通常トランザクション ログに記録される一般的なフィールドは、クライアントの要求が行われた日付と時刻、要求された URL、キャッシュ ヒットであったかキャッシュ ミスであったか、要求のタイプ、転送されたバイト数、およびソース IP アドレスです。

トランザクション ログは、通常、次のような目的で使用されます。

- 問題の特定と解決
- 負荷のモニタリング
- 課金請求
- 統計分析
- セキュリティ上の問題
- コスト分析とプロビジョニング

ACNS 5.2.1 ソフトウェア以降では、Windows Media Services 9 のロギングがサポートされています。Windows Media Services 9 Series では、Windows Media Services Version 4.1 よりもより強固なロギング モデルが提供されています。

事前定義済み形式（たとえば、Squid、Extended Squid、または Apache）または必要なフィールドをログに追加するカスタム トランザクション ログ形式で、データをログに残すことができます。トランザクション ログのコンテンツは定期的に外部サーバに FTP を使用してエクスポートできます。また、ログ ローテーション ポリシーを設定することもできます。

（注）　ロギング形式のタイプは、一度に 1 形式だけアクティブにできます。Content Engine GUI からトランザクション ロギングを有効にした場合は、Squid ログ形式が使用されます。

ACNS 5.x ソフトウェアはまたサニタイズド ロギングもサポートしています。サニタイズド ロギングが有効になっていると、Web リソース要求のロギングには Web クライアントの身元は含まれません（つまり不明になります）。トランザクション ログ ファイルのクライアントの IP アドレスとユーザ名は、偽装されています。詳細情報は、「トランザクション ログのサニタイジング」（P. 21-43）を参照してください。

ACNS 5.2 ソフトウェアでは、リモート syslog サーバに HTTP トランザクション ログ メッセージを送信する機能がサポートされています。この機能により、リモート syslog サーバ上で、HTTP 要求の認証失敗をリアルタイムで監視できます。詳細情報は、「HTTP 要求の認証失敗のリアルタイム モニタリング」（P. 21-49）を参照してください。ACNS 5.x ソフトウェアのトランザクション ログの詳細は、「スタンドアロン Content Engine 上でのトランザクションのモニタリング」（P. 21-28）を参照してください。

ACNS 5.2.3 ソフトウェア以降では、特定の URL のパフォーマンスを監視するように、Content Engine を設定することができます。Content Engine は、監視する URL 個々のさまざまな応答特性に関する統計情報を保持します。このトピックに関する詳細は、「スタンドアロン Content Engine 上でのクリティカル ディスク ドライブのモニタリング」（P. 21-18）を参照してください。